Pôle Universitaire Léonard de Vinci
ESI II 3906 – Cryptography

Semester 9 – Year 2009-2010
ESILV – Class of 2010

Problem Set 1

Working with GnuPG

Problem I

Generate a keypair with GnuPG and upload your key to the keyserver.

Problem II

Download the public key of at least two fellow classmates into your keyring.

1. Check the fingerprint of the key with them. Can you do such verification by e-mail?

2. Sign the public key you downloaded and upload it back into the keyserver.

Problem III

1. Send an encrypted and signed message to two of your fellow classmates.

2. Decipher two received encrypted messages.

Problem IV

1. Can you trust the public key with key ID 0x3A533CE1 belongs to Gaël Chareyron? Can you trust the statements contained in an e-mail sent by the owner of this key?

2. Can you trust the public key with key ID 0x54BFA094 belongs to Ronald Rivest[1]? Can you trust the statements contained in an e-mail sent by the owner of this key?

Problem V

A good friend of yours sends you an e-mail to tell you he signed your GnuPG key with his. He requests that you return the favor. The keysever shows that friend's signature. In addition, he is really a good friend of yours and you know you can trust that person. Should you sign his key?

[1] Ronald Rivest, American cryptographer, is one of the inventors of the RSA algorithm (and the R of RSA). He is the inventor of encryption algorithms RC2, RC4, RC5, co-inventor of RC6, and inventor of the has functions MD2, MD4, MD5 and MD6.

Ronald L. Rivest (1947–)

Problem VI

Choose three fellow classmates to work with you on this problem. Do not approach them with the request to work with you. Your three classmates will be named Alice, Bob and Charlie. For the sake of efficiency, it is suggested that e-mails sent in connection with this problem have "Problem 5" in the subject line.

Decide who will be Alice, Bob and Charlie. The point of the problem is to get this secret message to Charlie:

```
I chose you as classmate Charlie for Problem 5.
I am [your name and e-mail address].
Code is [choose a secret code].
Confirm receipt by sending me a signed-encrypted e-mail with the secret code.
```

The problem would be simple if you could send an e-mail to Charlie, however you should comply with these four requirements:

i) You are not allowed to contact Charlie directly. You are only allowed to send e-mails to Alice and Bob.

ii) Charlie should be sure the message has not been tampered with.

iii) You do not want Alice or Bob to know that you are contacting Charlie nor to have access to the secret message.

iv) The keys used in this problem must have been first uploaded to the keyserver and the name of the owner should be present on the key

It is assumed that Alice and Bob will comply with your requests. They will not share information with one another, unless you ask them to.

You succeeded if you receive a signed-encrypted message from Charlie confirming receipt of your communication (with your secret code) and no message from Alice or Bob notifying you they have discovered you have contacted Charlie (even if they do not know the content of the message). If you fail, redo the exercise after choosing a new Alice, a new Bob and a new Charlie.

Notes to Alices, Chalies and Bobs:

- If you are someone else's Charlie's, confirm receipt of the communication by sending a signed-encrypted e-mail to the originator of the message with the secret code.
- If you are someone else's Alice or Bob's, comply with the sender's request. Try to find out who is the originator *and* final recipient of the message. If you figure it out send a signed-encrypted e-mail to both of them and explain how you found out.